AMENDMENTS TO THE SPECIFICATION:

Please amend the paragraph beginning at page 9, line 22 as follows:

a second processing unit configured to obtain a residue number system representation of a value $Cq^{dq} \times B \bmod q$ or a value with q added thereto based on a residue number system representation of a remainder value $Cq = C \bmod q$ by q of the data C and a remainder value $dq = d \bmod$ [[(p - 1)]] (q - 1) by (q - 1) of the parameter d;